IN THE CLAIMS:

1-23. (cancelled)

24. (currently amended) A method for printing of sensitive data, comprising the steps of:

at a workstation encrypting sensitive data to be printed;

transferring to a printing device having a printing unit the encrypted sensitive data to be printed;

decrypting the sensitive data to be printed to create decrypted sensitive data;

converting the decrypted sensitive data to be printed into control signals for activation of the printing unit;

not storing the decrypted sensitive data in a readable decrypted form after the decrypting but before printing of the data, but rather storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory where a relationship of the memory segments in the non-volatile memory is stored in a volatile memory as relationship data independently of the stored decrypted sensitive data; and

printing the decrypted sensitive data with the printing unit on a recording medium.

25. (previously presented) A method of claim 24 wherein said decrypted sensitive data is stored in said non-volatile memory as said control signals representing said decrypted sensitive data.

26. (previously presented) A method of claim 24 including the step of relating the memory segments using said relationship data and then printing the decrypted sensitive data.

27. (cancelled)

28. (previously presented) A method according to claim 24 wherein the control signals containing decrypted sensitive data are stored in a volatile memory.

29. (previously presented) A method according to claim 24 wherein the decryption and the conversion into control signals are executed in immediate temporal succession.

30. (previously presented) A method according to claim 24 wherein the decryption and the conversion into control signals is executed in a controller for activation of a character generator.

31. (previously presented) A method according to claim 24 wherein print data are provided comprising both said sensitive data and non-sensitive data.

32. (previously presented) A method according to claim 31 wherein the print data to be printed are transferred to the printing device in the form of a print data stream, the print data stream being converted into an intermediate language in the printing device, and the print data being converted into control signals.

33. (previously presented) A method according to claim 31 wherein the sensitive data and the non-sensitive data are connected into one data unit before transfer to the printing device.

34. (previously presented) A method according to claim 33 wherein the sensitive data are identified in the data unit via markings.

35. (previously presented) A method according to claim 33 wherein a layout that comprises regions to receive sensitive data is generated using the non-sensitive data.

36. (previously presented) A method according to claim 33 wherein the sensitive data are already encrypted before combination with the non-sensitive data into said one data unit.

37. (previously presented) A method according to claim 33 wherein the sensitive data are encrypted after combination with the non-sensitive data into said one data unit.

38. (previously presented) A method according to claim 37 wherein only the sensitive data are encrypted.

39. (previously presented) A method according to claim 37 wherein both the sensitive data and the non-sensitive data are encrypted.

40. (previously presented) A method according to claim 24 wherein the conversion of the sensitive data to be printed into control signals for activation of the printing unit via rastering of the data to be printed into one or more raster images is executed, whereby the raster images represent the control signals.

41. (currently amended) A system for printing sensitive data which have been encrypted, comprising:

a printing device having a printing unit connected to a controller, said controller receiving said encrypted sensitive data;

said controller comprising a decryption module, a non-volatile memory, a relationship data volatile memory, and a converter which converts decrypted sensitive data from said decryption module into control signals for activation of said printing unit; and

in said controller not storing the decrypted sensitive data in a readable decrypted form after the decrypting, but before printing of the data, but rather storing the decrypted sensitive data in said non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory, and wherein a relationship of the memory segments in the non-volatile memory is stored as relationship data in said relationship data memory independently of the stored decrypted sensitive data.

42. (previously presented) A system of claim 41 wherein said decrypted sensitive data is stored in said non-volatile memory as said control signals representing said decrypted sensitive data.

43. (previously presented) A method of claim 41 wherein the controller relates the memory segments using said relationship data for printing the decrypted sensitive data.

44. (cancelled)

45. (previously presented) A system according to claim 41 wherein the printing unit comprises a character generator.

46. (previously presented) A system according to claim 41 wherein the controller comprises at least one raster module as said converter.

47. (previously presented) A system according to claim 41 wherein the controller comprises a combined decryption/raster module.

48. (previously presented) A system according to claim 41 wherein the controller comprises volatile storage media.

49. (previously presented) A system according to claim 41 wherein a sensor for detection of recording media with predetermined security features is arranged on a transport path for recording media in a region before the printing unit such that the printing of sensitive data can be stopped given detection of recording media without security features.

50. (cancelled)